DISTRIBUTED ARCHITECTURE FOR STATISTICAL OVERLOAD CONTROL AGAINST DISTRIBUTED DENIAL OF SERVICE ATTACKS

ABSTRACT

In a network including a centralized controller and a plurality of routers forming a security perimeter, a method for selectively discarding packets during a distributed denial-of-service (DDoS) attack over the network. The method includes aggregating victim destination prefix lists and attack statistics associated with incoming packets received from the plurality of routers to confirm a DDoS attack victim, and aggregating packet attribute distribution frequencies for incoming victim related packets received from the plurality of security perimeter routers. Common scorebooks are generated from the aggregated packet attribute distribution frequencies and nominal traffic profiles, and local cumulative distribution function (CDF) of the local scores derived from the plurality of security perimeter routers are aggregated. A common discarding threshold is derived from the CDF and sent to each of the plurality of security perimeter routers, where the discarding threshold defines a condition in which an incoming packet may be discarded at the security perimeter.